UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/536,577	03/28/2000	Curtis Lee Cornils	IRI05247	5755

22863 7590 05/06/2004

MOTOROLA, INC.
CORPORATE LAW DEPARTMENT - #56-238
3102 NORTH 56TH STREET
PHOENIX, AZ 85018

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	5

DATE MAILED: 05/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/536,577	CORNILS ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. In response to the first office action, Applicant has submitted a Request for Reconsideration and a substitute specification on 30 March 2004.

2. Claims 1-15 have been examined.

Specification

3. The replacement specification is acceptable.

Claim Rejections - 35 USC § 102

4. Claims 8-11 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,584,566 to Hardjono.

As per claims 8 and 9, the group key management method disclosed by Hardjono process for re-keying upon a member leaving (regardless of the reason for the member leaving the group) wherein a key encryption key (SGK) is used to encrypt new key information being multicasted to other top-tier servers or sent one at a time (see column 8, line 45 to column 9, line 16).

As per claims 10 and 11, new sets of keys are sent to all but the compromised node (see column 9, lines 23-42).

5. Claims 12-15 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,592,552 to Fiat.

The Broadcast Encryption method disclosed by Fiat includes a hierarchy of encryption keys, with keys assigned to nodes at each level (see column 12, line 58 to column 13, line 10).

Claim Rejections - 35 USC § 103

6. Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,584,566 to Hardjono as applied to claims 8-11 above, and further in view of U.S. Patent No. 6,684,334 to Srivastava further in view of U.S. Patent No. 6,195,751 to Caronni et al.

Regarding claims 1 and 2, Hardjono only discloses a top-down key distribution in a two-tiered system. Since it is only advantageous to use recursive algorithms in systems having at least three tiers, no recursion is disclosed.

The broadcast encryption system disclosed by Srivastava uses more than two tiers in its hierarchy, and Srivastava further suggests that this reduces the number of keys affected by a change, reducing the workload on the group controller (see column 15, line 66 to column 16, line 59 and Figure 5).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Hardjono using more than two tiers, as disclosed by Srivastava, in order to reduce the workload on the group controller.

The multicasting system disclosed by Caronni distributes keys in a recursive manner (by rebroadcasting) in order to ensure that new keys are distributed to participants that do not share common key encryption keys with a participant that generates new keys (see column 14, line 55 to column 15, line 5).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Hardjono and Srivastava by recursively distributing new keys, as disclosed by Caronni, in order that new keys are distributed to participants that do not share common key encryption keys with a participant that generates new keys.

Regarding claim 3-5, since the algorithm is recursive, the key distribution within lower tiers would be as in manner disclosed for the top tier as disclosed by Hardjono.

As per claim 6, the system disclosed by Hardjono may be used in an infrared (i.e. wireless) system (see column 4, line 1).

As per claim 7, the system disclosed by Hardjono may be used with the Internet (see column 4, line 6).

Response to Arguments

7. Regarding claims 8-15, Applicant's arguments filed 30 March 2004 have been fully considered but they are not persuasive.

In response to applicant's argument with respect to the rejection of claims 8-15 under 35 U.S.C. 102 that the references fail to show certain features of applicant's

invention, it is noted that the features upon which applicant relies are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Regarding claims 8-11, a tier is simply a level within a hierarchy, and the top tier, therefore, is a hierarchy's highest level. One cannot construe from the claims as written that the hierarchy have a particular size or structure. The procedure disclosed by Hardjono teaches to the replacement a keys with respect to a particular key server for any reason (including the compromising of a node); since Hardjono, in the procedure of column 8, lines 45-49, discloses the notification of the other servers (i.e. the ones not having the compromised node) in a group, it is inherent that it must reference a list of servers in order to determine what those servers would be. The servers notified exist at the upper level. The technique used by Hardjono clearly anticipates the claimed encryption of the new traffic encryption key, and it is sent out via multicast, which is a form of broadcast.

Regarding claims 12-15, Fiat discloses the keys being stored in all of the non-leaf nodes of a tree structure and the corresponding nodes being in the leaves, which constitutes a hierarchy that reads to all of the claims. It is stated throughout Fiat's specification that all of the keys are simultaneously in storage (see column 1, lines 65-57, for example) and it is therefore inherent that the invention disclosed by Fiat includes a storage device that is separate from the encryption means.

8. Regarding claims 1-7, Applicant's arguments, see Paper No. 4, filed 30 March 2004, with respect to the rejections of claims 1-7 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground of rejection is made in view of U.S. Patent No. 6,584,566 to Hardjono as applied to claims 8-11 above, and further in view of U.S. Patent No. 5,592,552 to Fiat further in view of U.S. Patent No. 6,195,751 to Caronni et al., as described above.

Hardjono discloses a two-tiered hierarchy. In such a case, all lower nodes in the hierarchy are directly connected to a node in the upper tier; therefore, no provision has to be made for the situation where the broadcasts from the top-tier nodes doesn't reach a leaf because it is not directly connected.

The technique of recursion is a common method for reaching a nodes in a structure that are not directly connected to any nodes residing in a particular group, and it is this need that is addressed by the combining of Caronni. Though the layout of nodes in not necessarily hierarchical, the recursive algorithm disclosed with respect to the transmission of keys is analogous.

Nonetheless, the there would be no reason to incorporate a recursive algorithm unless there existed more than two tiers. The grounds for rejection have therefore been changed.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday-Thursday from 8:00 AM - 4:00 PM Eastern Time. The examiner can also be reached on alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(703) 872-9306
Hand-delivered responses should be brought to Crystal Park 2, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

MEH

April 28, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100